

# Capstone Final Report- PGPCS-UTA June 2023

## <Wenshan, Liu>

### Objectives completed:

- Task 1 – Wazuh Installation and Configuration
- Task 2 – Wazuh Agent Installation and Configuration
- Task 3 – Acquiring Authentication Failure Logs
- Task 4 – Generating report for Authentication Failure Logs
- Task 5 – Setting Up Wazuh File Integrity Monitoring
- Task 6 – Generating Report for File Integrity Management
- Task 7 – Detecting Vulnerabilities in Windows Machine
- Task 8 – Analyzing the Vulnerability Dashboard

## Implementation:

- Task 1 – Wazuh Installation and Configuration

In this task, the Wazuh server would be installed on a Linux system. Here is a screenshot of the successful installation. At the same time, check the IP address, and this machine will be investigated later.



To make sure the server can work appropriately. The services should be started with root user privilege. Thus, use the command “**sudo su**” and enter the password for Wazuh-user as wazuh.

```
[root@wazuh-server wazuh-user]# sudo systemctl enable wazuh-manager
[root@wazuh-server wazuh-user]# sudo systemctl start wazuh-manager
[root@wazuh-server wazuh-user]#
```

```
[wazuh-user@wazuh-server ~]$ sudo systemctl enable wazuh-indexer
[wazuh-user@wazuh-server ~]$ sudo systemctl start wazuh-indexer
[wazuh-user@wazuh-server ~]$
```

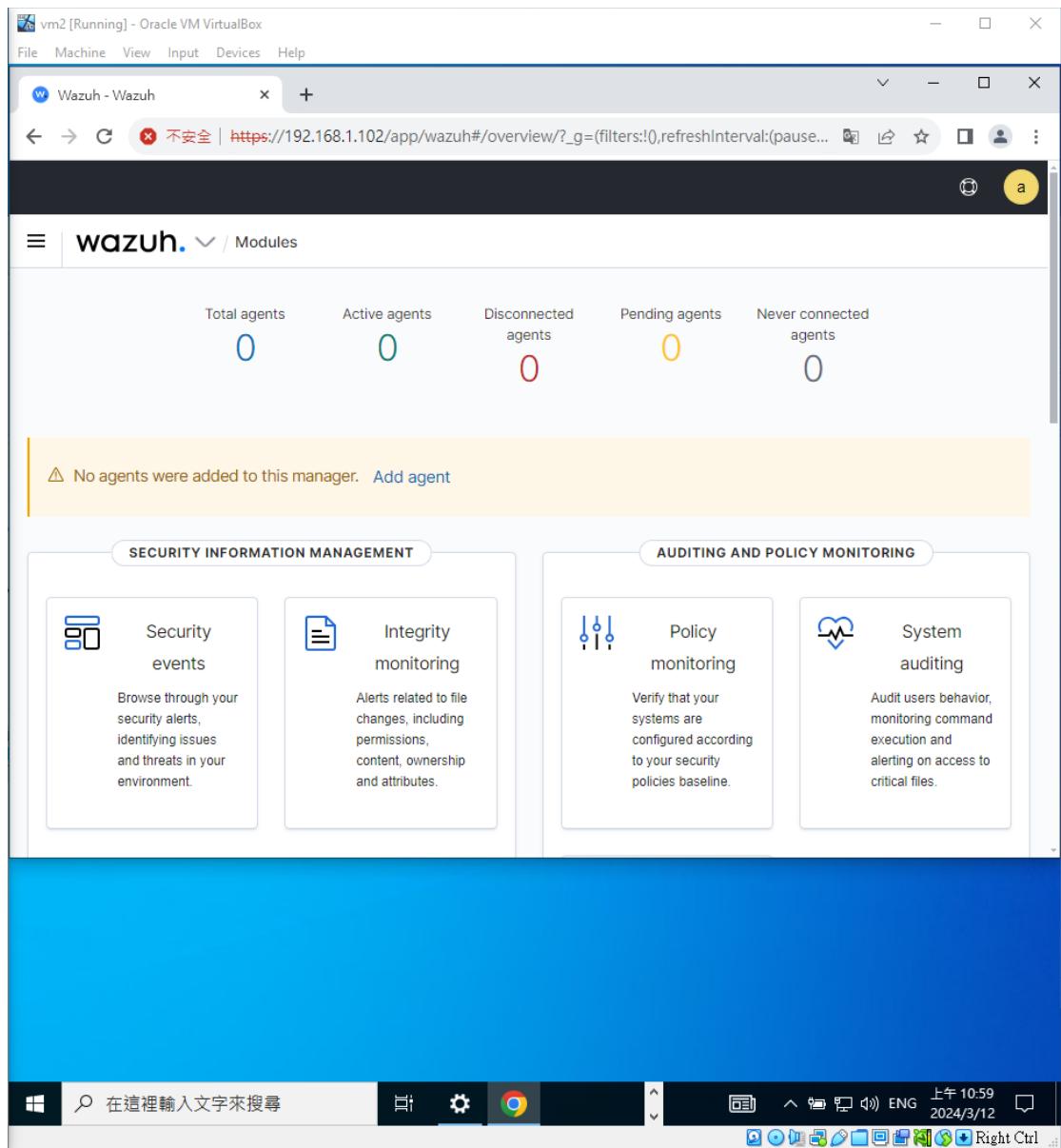
```
[root@wazuh-server wazuh-user]# sudo systemctl enable wazuh-dashboard
[root@wazuh-server wazuh-user]# sudo systemctl start wazuh-dashboard
[root@wazuh-server wazuh-user]#
```

Ensure that the service is working. The command "systemctl" may verify this.

```
File Machine View Input Devices Help

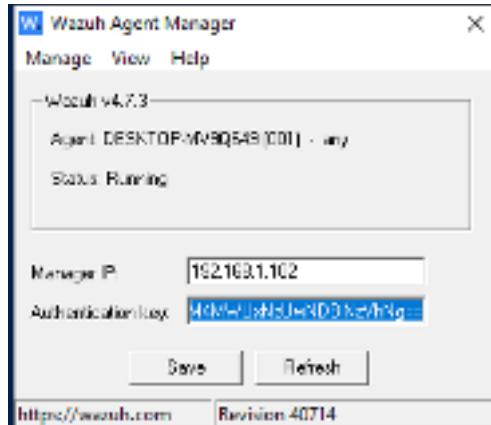
rhel-dmesg.service          loaded active exited   Dump dmesg to /var/log/dmesg
rhel-domainname.service      loaded active exited   Read and set NIS domainname from /etc/
rhel-readonly.service        loaded active exited   Configure read-only root support
rpcbind.service              loaded active running  RPC bind service
rsyslog.service              loaded active running  System Logging Service
sshd.service                 loaded active running  OpenSSH server daemon
systemd-journal-fflush.service loaded active exited   Flush Journal to Persistent Storage
systemd-journald.service     loaded active running  Journal Service
systemd-logind.service       loaded active running  Login Service
systemd-random-seed.service  loaded active exited   Load/Save Random Seed
systemd-remount-fs.service   loaded active exited   Remount Root and Kernel File Systems
systemd-sysctl.service       loaded active exited   Apply Kernel Variables
systemd-tmpfiles-setup-dev.service loaded active exited   Create Static Device Nodes in /dev
systemd-tmpfiles-setup.service loaded active exited   Create Volatile Files and Directories
systemd-udev-trigger.service loaded active exited   udev Coldplug all Devices
systemd-udevd.service        loaded active running  udev Kernel Device Manager
systemd-update-utmp.service  loaded active exited   Update UTMP about System Boot/Shutdown
systemd-user-sessions.service loaded active exited   Permit User Sessions
systemd-vconsole-setup.service loaded active exited   Setup Virtual Console
tuned.service                loaded active running  Dynamic System Tuning Daemon
vboxadd-service.service      loaded active running  vboxadd-service.service
vboxadd-service              loaded active exited   vboxadd-service
wazuh-dashboard.service      loaded active running  wazuh-dashboard
wazuh-indexer.service        loaded active running  Wazuh Indexer
wazuh-manager.service        loaded active running  Wazuh Manager
-.slice                      loaded active active   Root Slice
system-getty.slice           loaded active active   system-getty.slice
system-selinux\x2dpolicy\x2dmigrate\x2dlocal\x2dchanges.slice loaded active active   system-selinux
system.slice                 loaded active active   System Slice
user-1000.slice              loaded active active   User Slice of wazuh-user
user.slice                   loaded active active   User and Session Slice
dbus.socket                  loaded active running  D-Bus System Message Bus Socket
rpcbind.socket               loaded active running  RPCbind Server Activation Socket
systemd-initctl.socket      loaded active listening /dev/initctl Compatibility Named Pipe
systemd-journald.socket     loaded active running  Journal Socket
lines 36-71 quit
[root@wazuh-server wazuh-user]#
```

Next, power on the Windows machine and enter the IP of the Linux machine on the Wazuh server in the web browser. Here is a screenshot of logging in successfully.

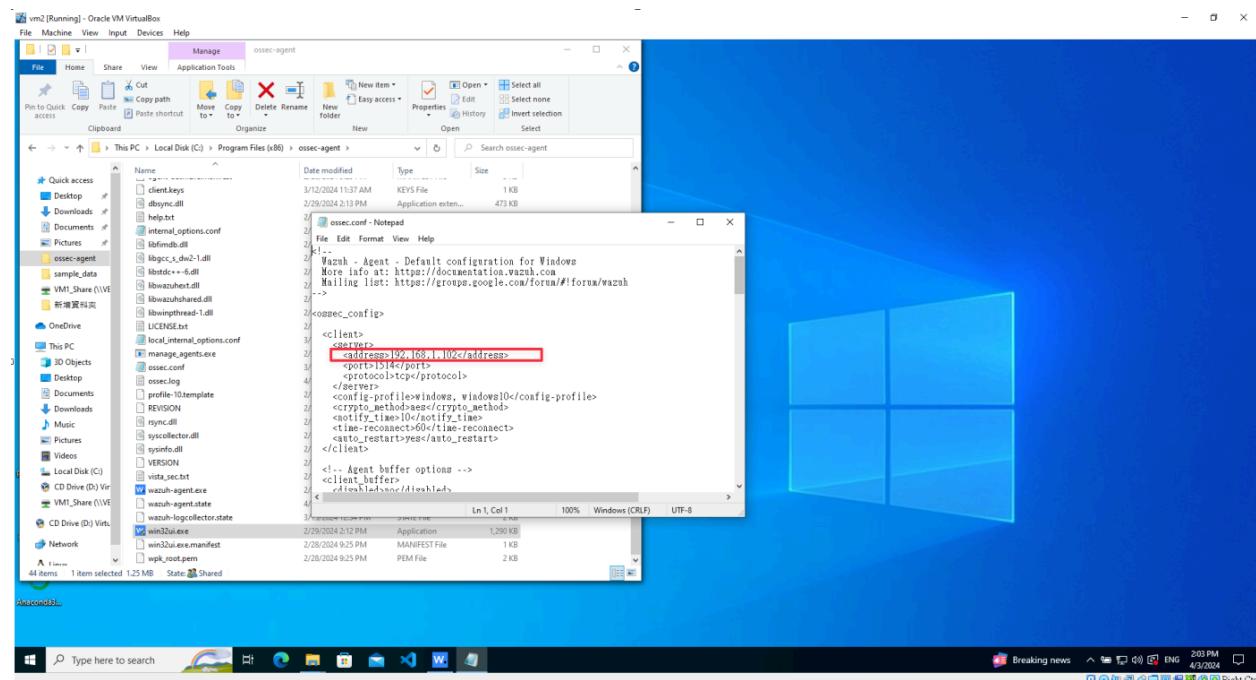


- Task 2 – Wazuh Agent Installation and Configuration

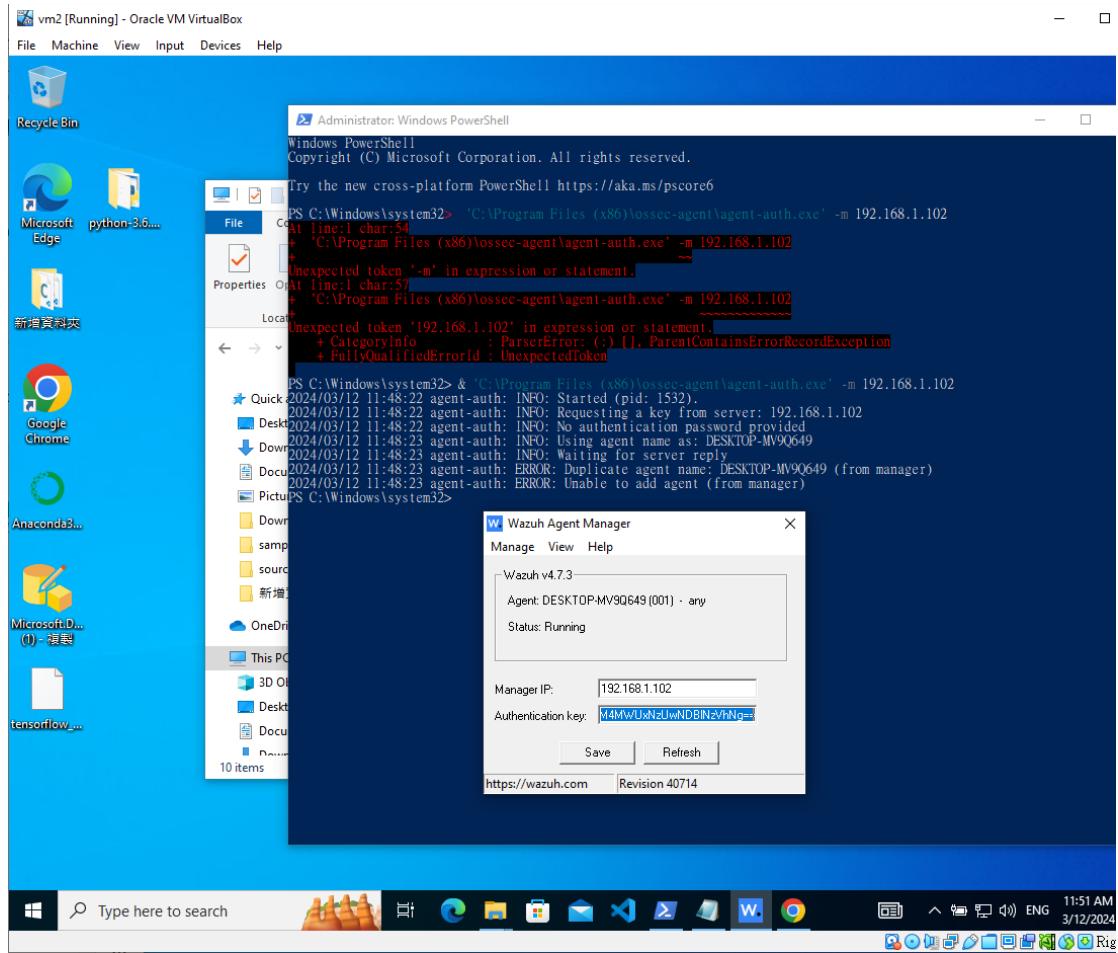
In task 2, the Wazuh agent would be installed on the Windows machine. Download and install wazuh-agent4.3.10-1.msi. After installed, open Win32ui.exe in C Drive> Program Files (X86) > ossec-agent path.



Next step, go to “View” -> “View Config” to adjust Wazuh’s IP address as seen in the Wazuh CLI.



Open Windows PowerShell to get a valid key. Command: “& ‘C:\Program Files (x86)\ossec-agent\agent-auth.exe’ -m <IP\_ADDRESS\_OF\_WAZUH> “



Then, go to 'Wazuh Agent Manager'-> 'Manage' -> 'Start.' In this step, it would restart the agent after a change.

Go to Wazuh Dashboard to verify the agent was added.

The screenshot shows the Wazuh web application running in a browser window titled 'Wazuh - Wazuh'. The URL is [https://192.168.1.102/app/wazuh#/agents?tab=welcome&agent=001&\\_g=\(filters:!\(\),refreshInterval:\(pause:!t,value:...](https://192.168.1.102/app/wazuh#/agents?tab=welcome&agent=001&_g=(filters:!(),refreshInterval:(pause:!t,value:...). The main content area displays agent information for 'DESKTOP-MV9Q649' (ID 001). The agent is active, with IP 192.168.1.84, Version Wazuh v4.7.3, and Group default. It is running on Microsoft Windows 10 Pro (node01). A circular chart titled 'Compliance' shows the distribution of rules across different levels: 2.2 (396), 2.2.5 (53), 4.1 (44), 10.6.1 (43), and 10.2.5 (28). On the left, a sidebar lists MITRE Top Tactics: Defense Evasion (24), Persistence (24), Initial Access (23), Privilege Escalation (23), and Impact (2). Below the chart is a table titled 'FIM: Recent events' with columns: Time, Path, Action, Rule ..., Rule Level, and Rule Id. The Windows taskbar at the bottom shows various pinned icons and the system tray.

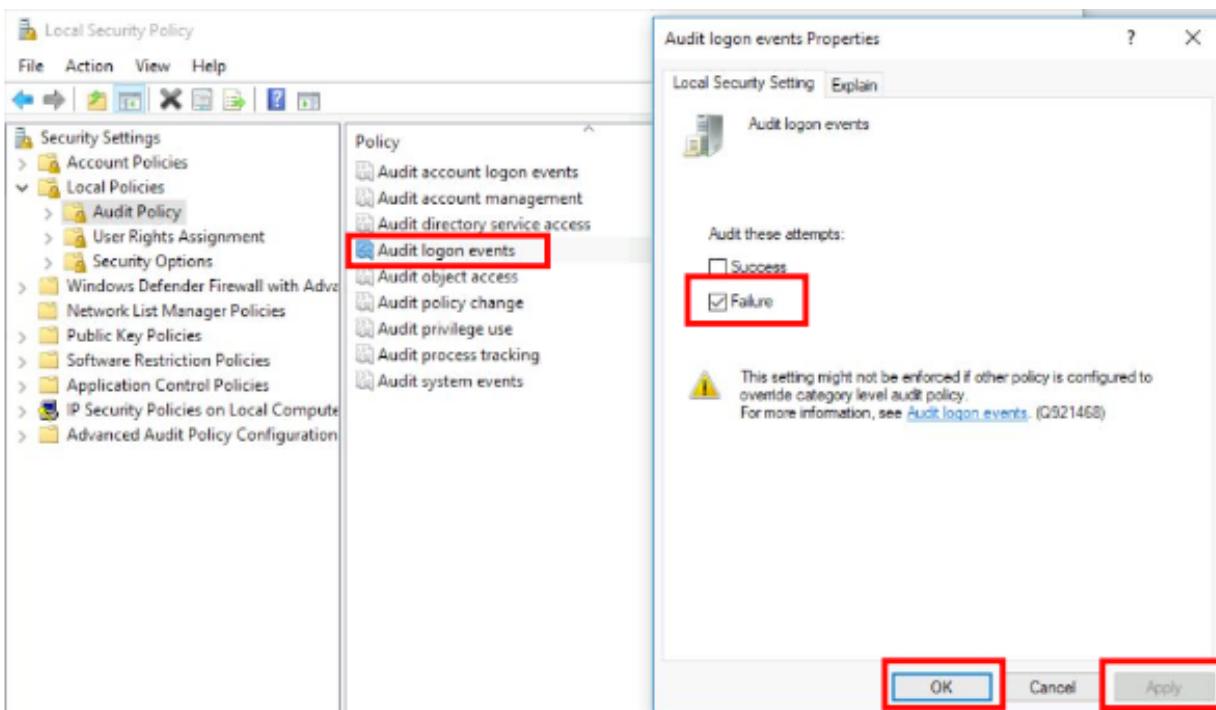
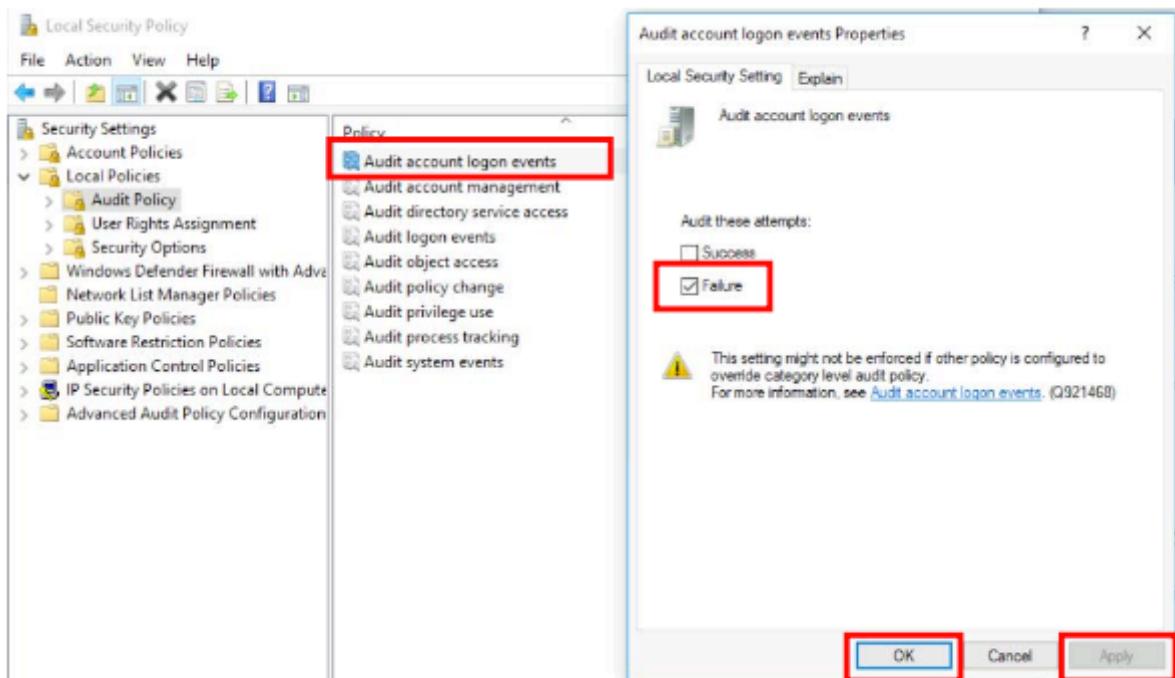
- **Task 3 – Acquiring Authentication Failure Logs**

In this task, I will give an example of how to get the authentication failure logs.

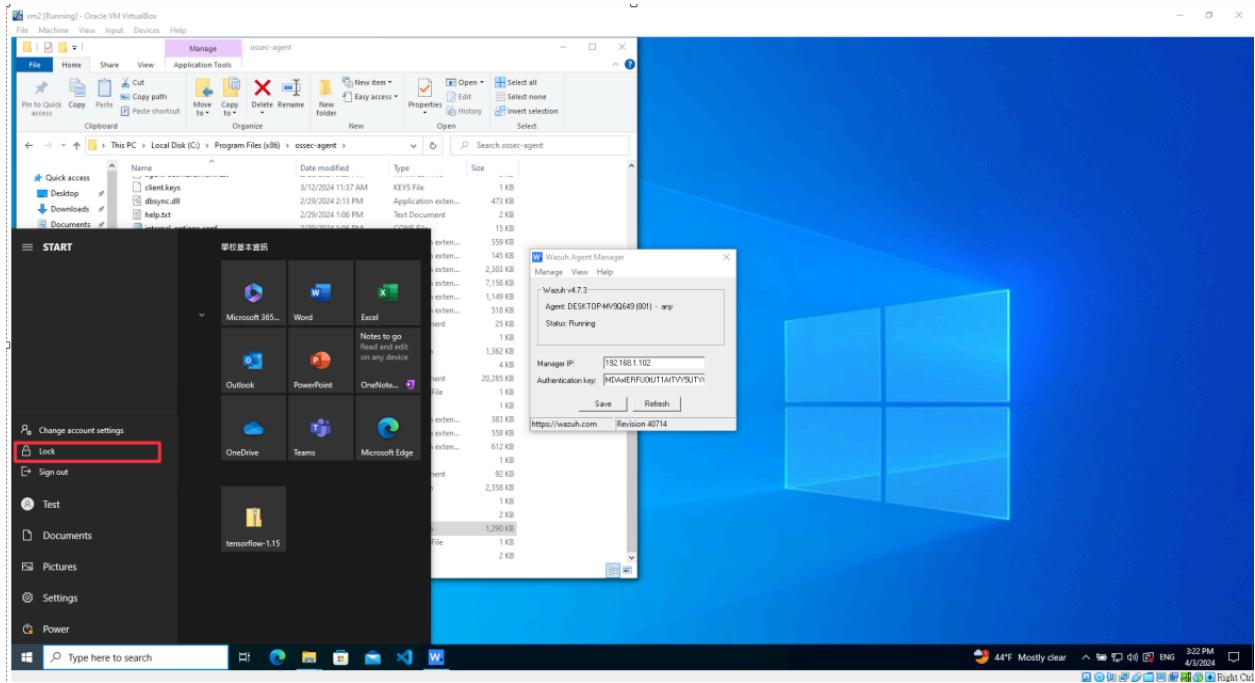
Firstly, on the Windows machine, go to ‘Local Security Policy’ -> ‘Local Policies’ -> ‘Audit Policy’ ->‘Audit account logon events’ -> click ‘Failure’ -> and click ‘Apply’ and ‘OK’.

Secondly, go to ‘Local Security Policy’ -> ‘Local Policies’ -> ‘Audit account logon events’.

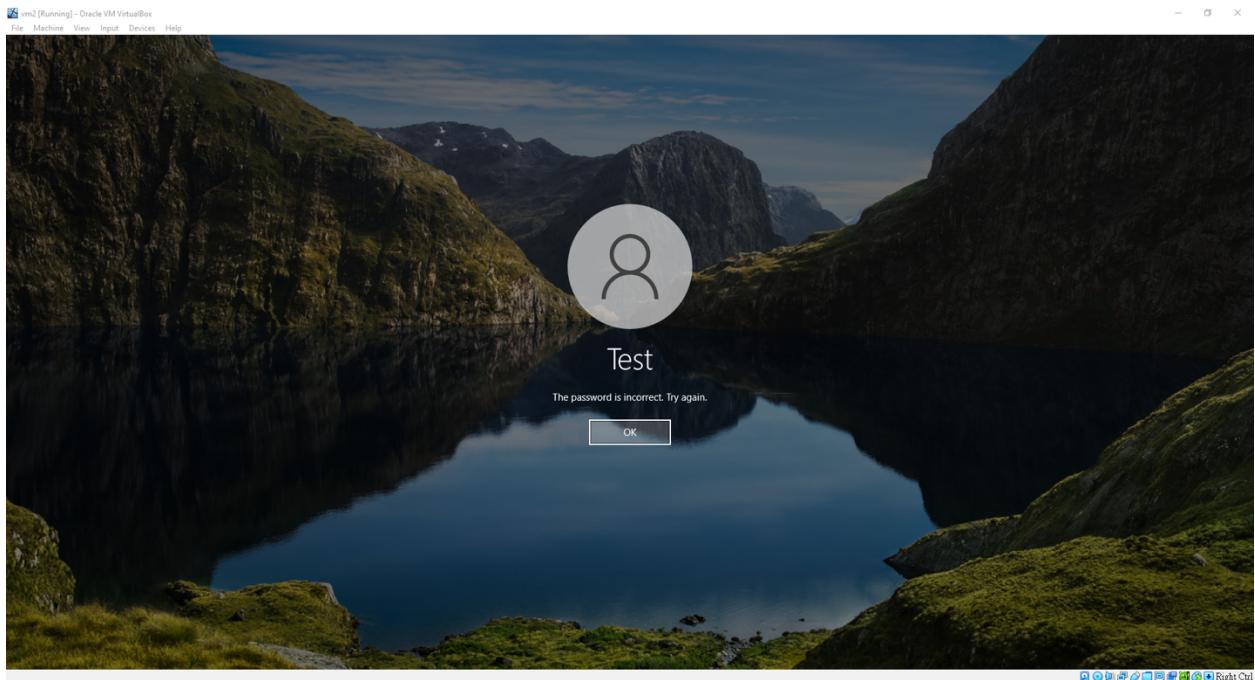
->‘Audit logon events’ -> click 'Failure', then click 'Apply' and 'OK'.



Third, lock the windows machine.



Try logging via incorrect passwords many times.



Finally, go to the Wazuh dashboard and click on "security events." The picture below displays the authentication failure logs.

The screenshot shows a Wazuh dashboard titled "wazuh" under "Security events". The main table displays several security alerts, with two specific entries highlighted by red boxes:

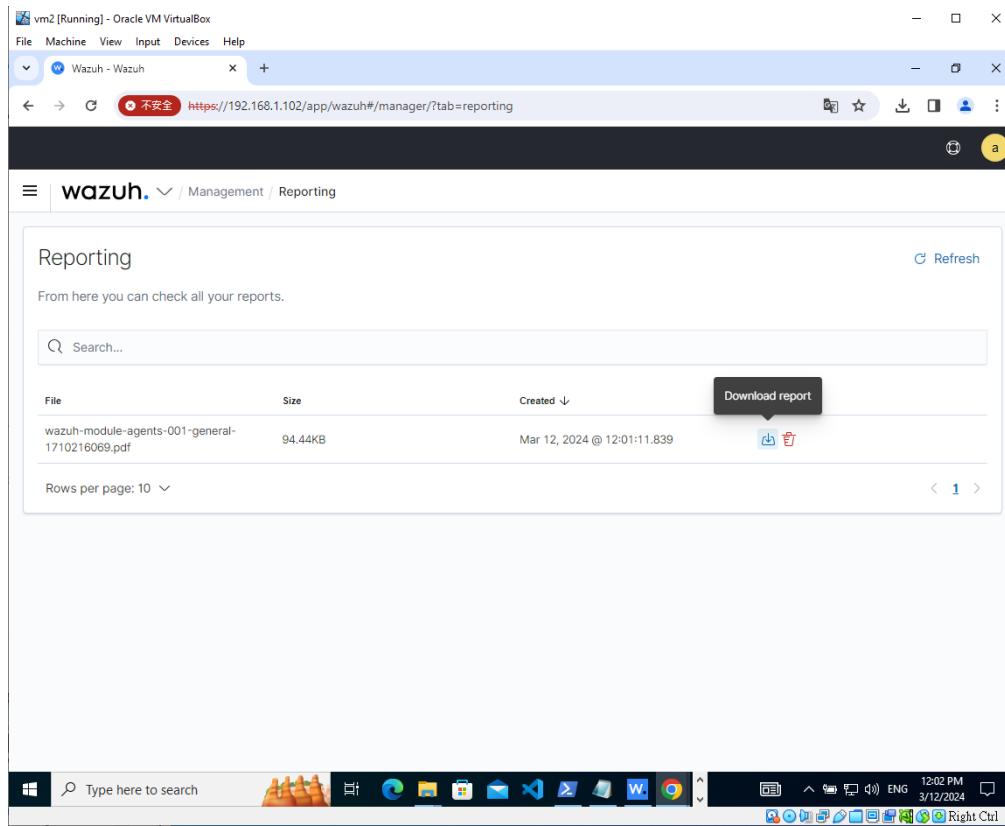
Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Mar 12, 2024 @ 11:57:32.472	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
Mar 12, 2024 @ 11:57:32.467			Windows audit failure event.	5	60104
Mar 12, 2024 @ 11:57:28.591	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
Mar 12, 2024 @ 11:57:28.587			Windows audit failure event.	5	60104
Mar 12, 2024 @ 11:57:12.247	T1098	Persistence	User account changed.	8	60110
Mar 12, 2024 @ 11:56:21.085			Software protection service scheduled successfully.	3	60642
Mar 12, 2024 @ 11:53:00.736			Windows audit policy changed.	8	60112
Mar 12, 2024 @ 11:53:00.713			Windows audit policy changed.	8	60112
Mar 12, 2024 @ 11:53:00.674			Windows audit policy changed.	8	60112

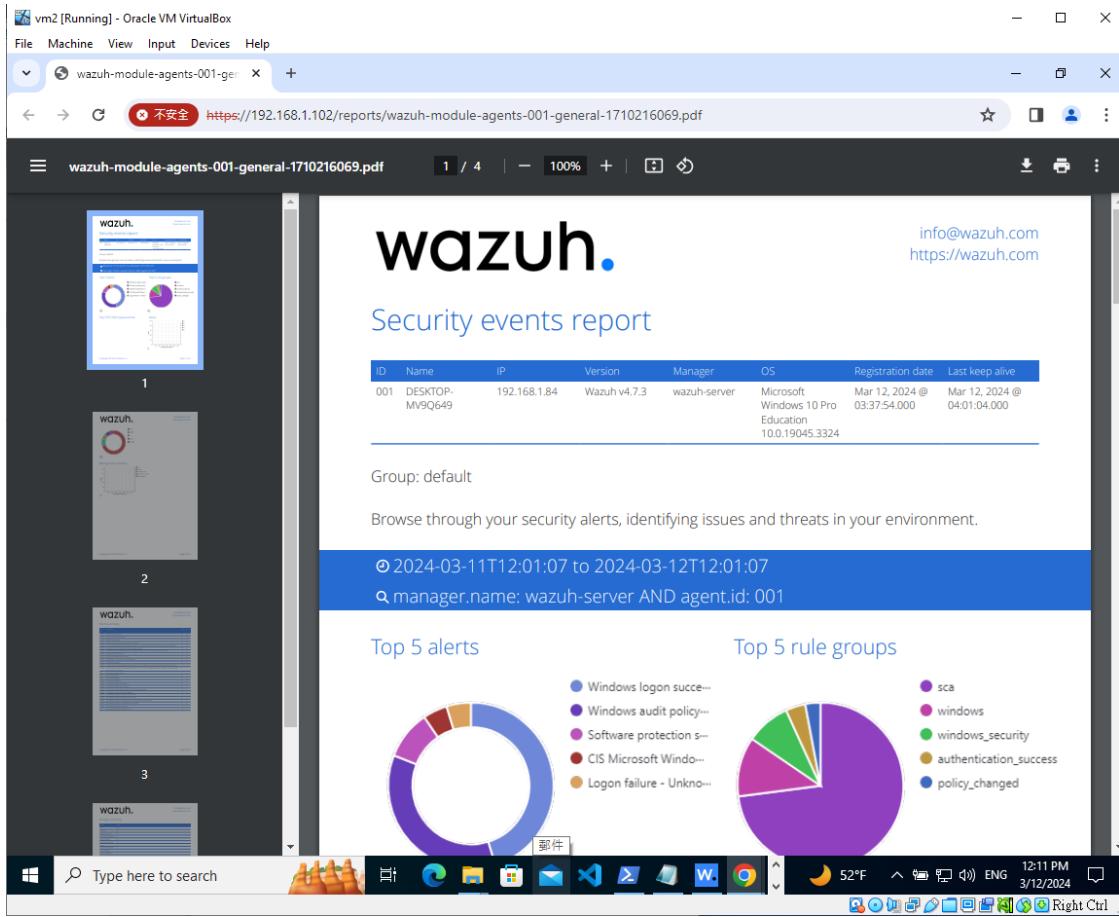
The dashboard also includes a search bar at the bottom and a taskbar with various icons and system status information.

- Task 4 – Generating report for Authentication Failure Logs

In this task, it is an example of how to generate reports for authentication failure logs.

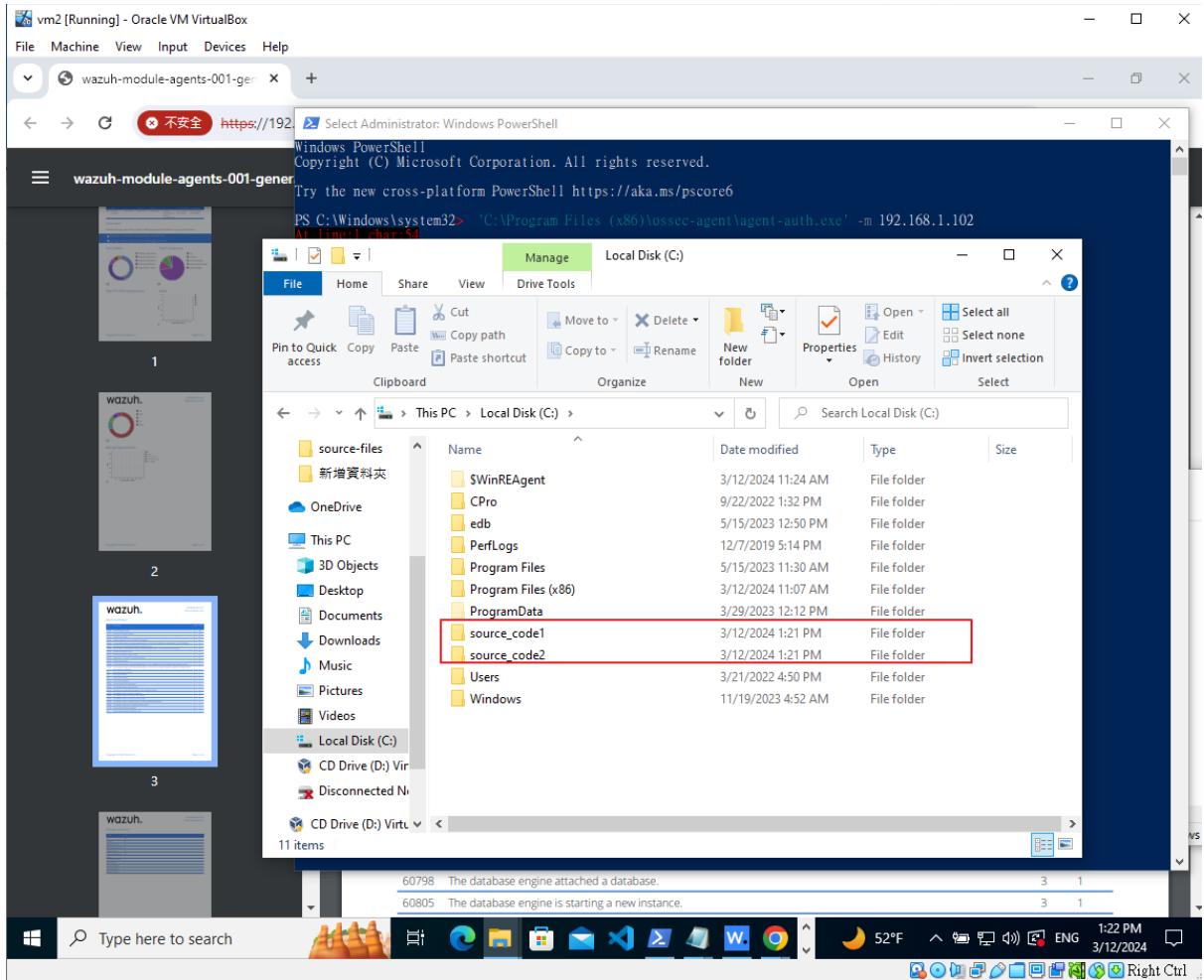
Open the authentication failure logs in the Wazuh dashboard -> 'generate report'. Go to 'Management >'Reporting'. Here will be the report that records the authentication failure.





- Task 5 – Setting Up Wazuh File Integrity Monitoring

In this task, it would need to create two folders that are monitoring targets. First, create two folders, “source\_code1” and "source\_code2," in C Drive.



Second, go to Wazuh Agent Manager -> 'View' -> 'View Config'.

Then, edit the config file. Delete the commands under <!-- File integrity monitoring -->. starting from <syscheck> to </syscheck>. [Ensure that you delete the commands in-between <!-- File integrity monitoring --> and <!-- System Inventory -->].

```

<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>
    ↓
  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <!-- Default files to be monitored. -->
  <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>

  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|n
  <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>
  <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>

  <!-- 32-bit programs. -->
  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|n
  <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
    ↑

  <!-- Frequency for ACL checking (seconds) -->
  <windows_audit_interval>60</windows_audit_interval>

  <!-- Nice value for Syscheck module -->
  <process_priority>10</process_priority>

  <!-- Maximum output throughput -->
  <max_eps>100</max_eps>

  <!-- Database synchronization settings -->
  <synchronization>
    <enabled>yes</enabled>
    <interval>5m</interval>
    <max_interval>1h</max_interval>
    <max_eps>10</max_eps>
  </synchronization>
</syscheck>
  ↑
<!-- System inventory -->
  <bundle_name>syscollector</bundle_name>

```

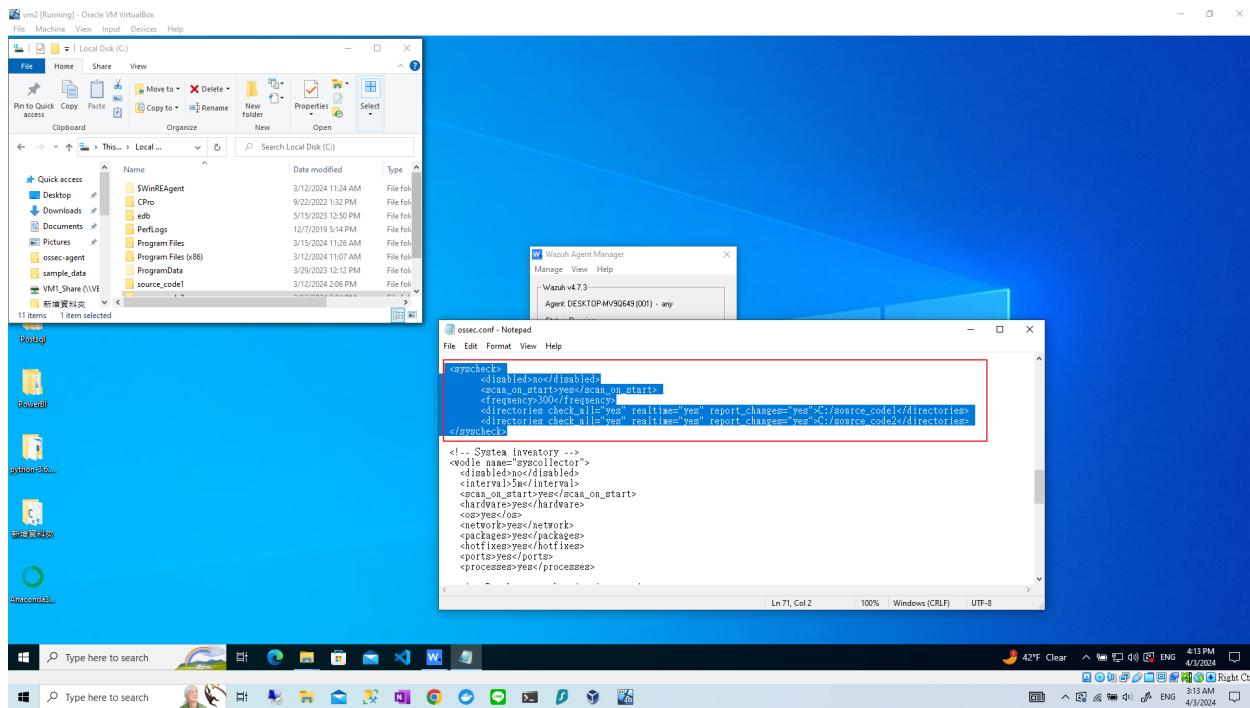
After deleting the default file integrity monitoring command, paste/type the below command under “<!-- File integrity monitoring -->”.

```

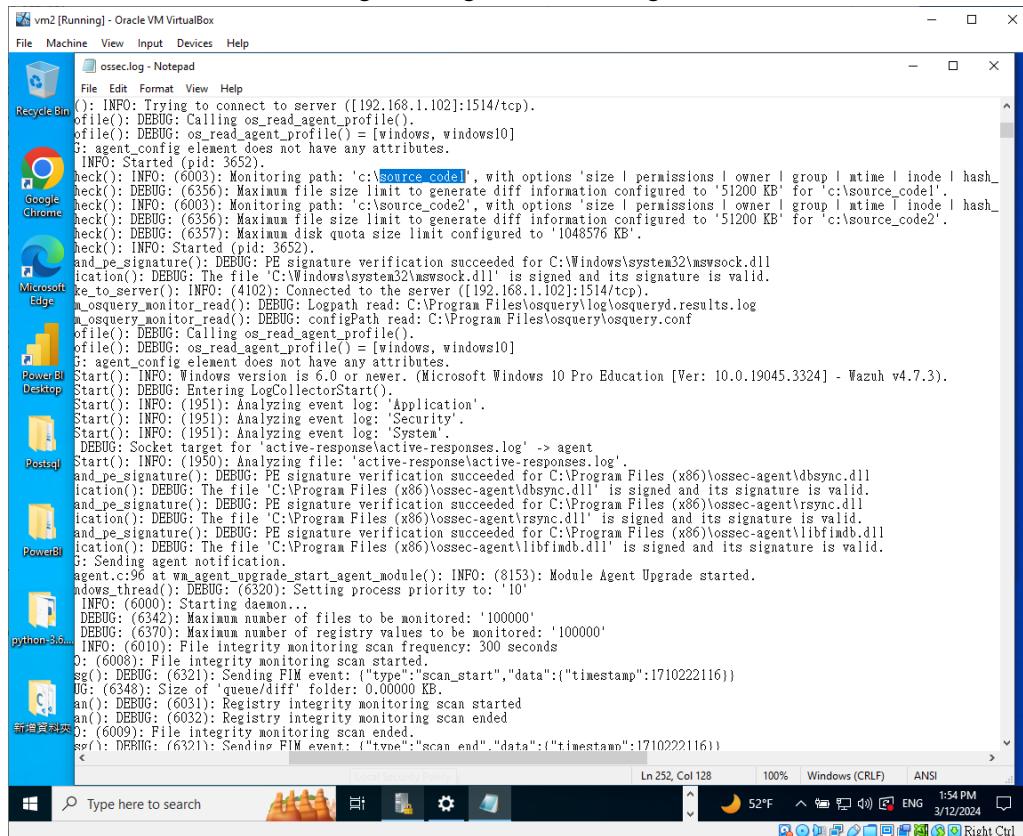
<syscheck>
<disabled>no</disabled>
<scan_on_start>yes</scan_on_start>
<frequency>300</frequency>
<directories check_all="yes" realtime="yes"
report_changes="yes">C:/source_code1</directories> <directories check_all="yes"
realtime="yes" report_changes="yes"> C:/source_code2</directories>

</syscheck>

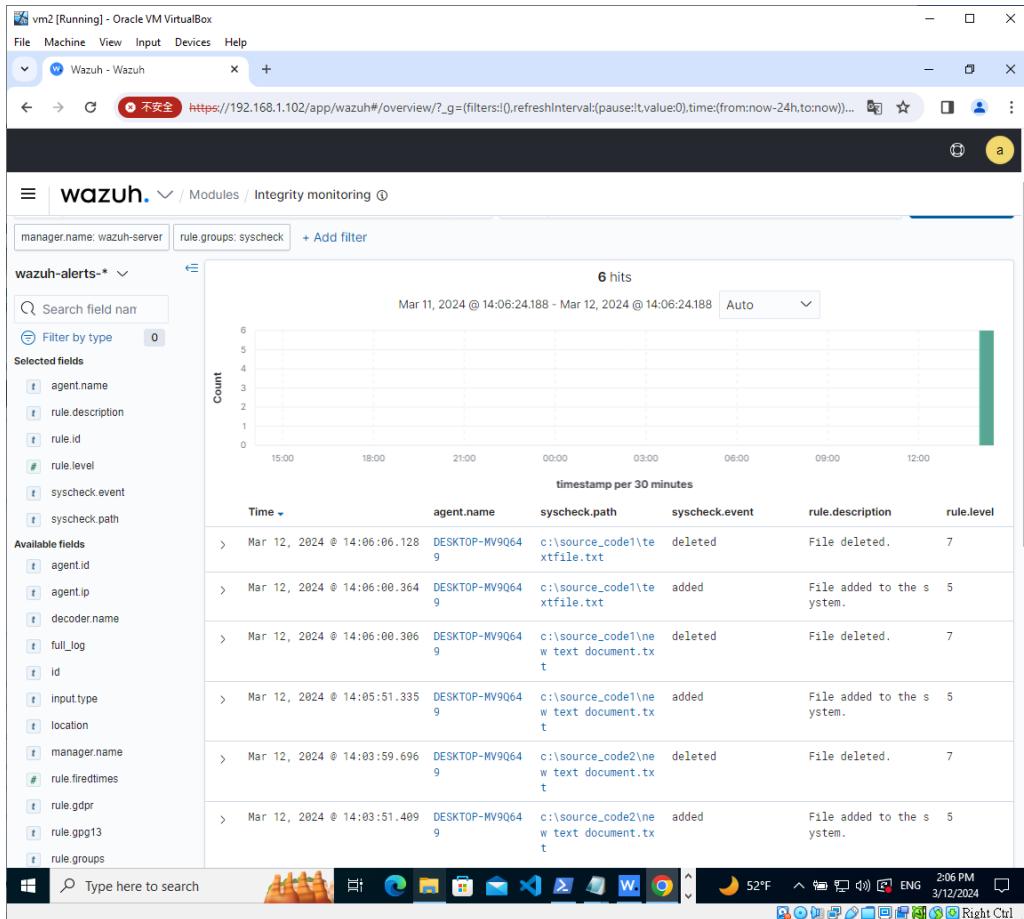
```



Third, save the ‘View Config’, then go to ‘View Logs’. Check if the file is monitored.

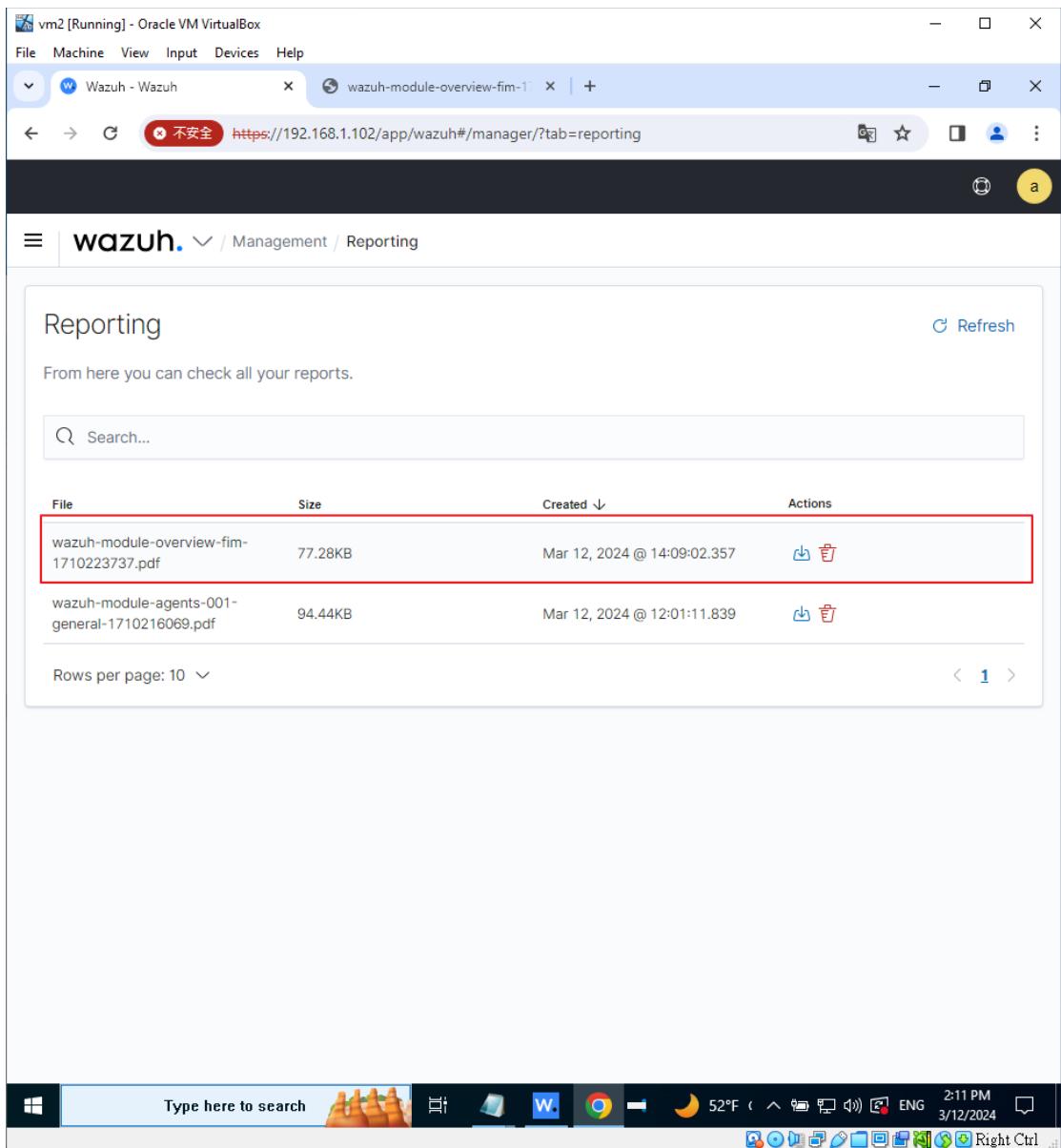


Last, go to the Wazuh dashboard and click on Integrity Monitoring. Here, it shows the operation of the folders 'source\_code1' and 'source\_code2'.



- Task 6 – Generating Report for File Integrity Management

In this task, it is same as the task4. Open the Wazuh dashboard ->'Integrity Monitoring' ->'Generate Report'.



- Task 7 – Detecting Vulnerabilities in Windows Machine.

In this task, it would show how to use Wazuh to detect vulnerabilities in Windows machines.

First, open the Wazuh dashboard. Click on -> 'Management' -> 'Configuration'.

The screenshot shows the Wazuh web interface. In the top left, there's a sidebar with icons for Modules, Management, Agents, Tools, Security, and Settings. The 'Management' icon is highlighted with a red box. The main content area has three columns: 'Management directory' (with sub-links for Administration, Rules, Decoders, CDB lists, Groups, and Configuration), 'Status and reports' (with sub-links for Status, Cluster, Statistics, Logs, and Reporting), and a summary section on the right showing 'Never connect agents' (0) and a 'MONITORING AND POLICY MONITORING' section with a heart rate icon.

Second, Click on “Edit Configuration”.

The screenshot shows the 'Configuration' management page. At the top, there's a 'Refresh' button, an 'Edit configuration' button (which is highlighted with a red box), and a help icon. Below this, there are two sections: 'Main configurations' and 'Alerts and output management'. The 'Main configurations' section lists four items: Global Configuration (Global and remote settings), Cluster (Master node configuration), and Registration Service (Automatic agent registration service). The 'Alerts and output management' section lists two items: Alerts (Settings related to the alerts and their format) and Integrations (Slack, VirusTotal and PagerDuty integrations with external APIs).

Third, edit the configuration. After edit, save the file.

## Manager configuration

[Refresh](#)[Save](#)[Restart Manager](#)

### Edit ossec.conf of Manager

```
100  <scan_on_start>yes</scan_on_start>
101  <interval>12h</interval>
102  <skip_nfs>yes</skip_nfs>
103  </sca>
104
105  <vulnerability-detector>
106  | <enabled>yes</enabled>
107  | <interval>2m</interval>
108  | <min_full_scan_interval>5m</min_full_scan_interval>
109  | <run_on_start>yes</run_on_start>
110
111  <!-- Ubuntu OS vulnerabilities -->
112  <provider name="canonical">
113  | <enabled>yes</enabled>
114  | <os>trusty</os>
115  | <os>xenial</os>
116  | <os>bionic</os>
117  | <os>focal</os>
118  | <os>jammy</os>
119  | <update_interval>1h</update_interval>
```

## Manager configuration

[Refresh](#)[Save](#)[Restart Manager](#)

### Edit ossec.conf of Manager

```
156  | <os>15-server</os>
157  | <os>15-desktop</os>
158  | <update_interval>1h</update_interval>
159  | </provider>
160
161  <!-- Arch OS vulnerabilities -->
162  <provider name="arch">
163  | <enabled>yes</enabled>
164  | <update_interval>1h</update_interval>
165  | </provider>
166
167  <!-- Windows OS vulnerabilities -->
168  <provider name="msu">
169  | <enabled>yes</enabled>
170  | <update_interval>2m</update_interval>
171  | </provider>
172
173  <!-- Aggregate vulnerabilities -->
174  <provider name="nvd">
175  | <enabled>yes</enabled>
176  | <update_from>https://nvd.cisa.gov/nvd/jsonfeed/nvdcve-1.1.json</update_from>
```

wazuh. Management / Configuration

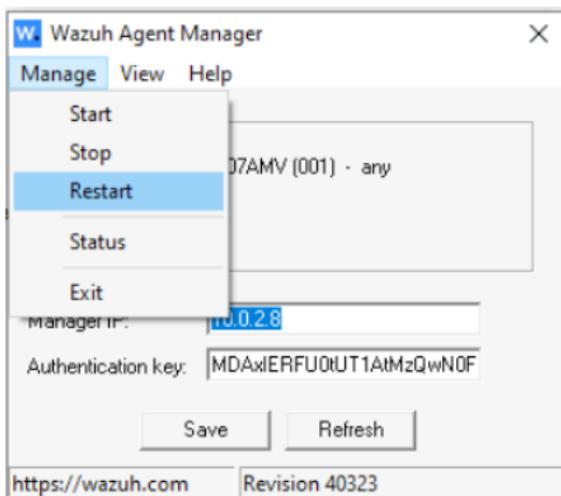
### Manager configuration

Edit ossec.conf of Manager

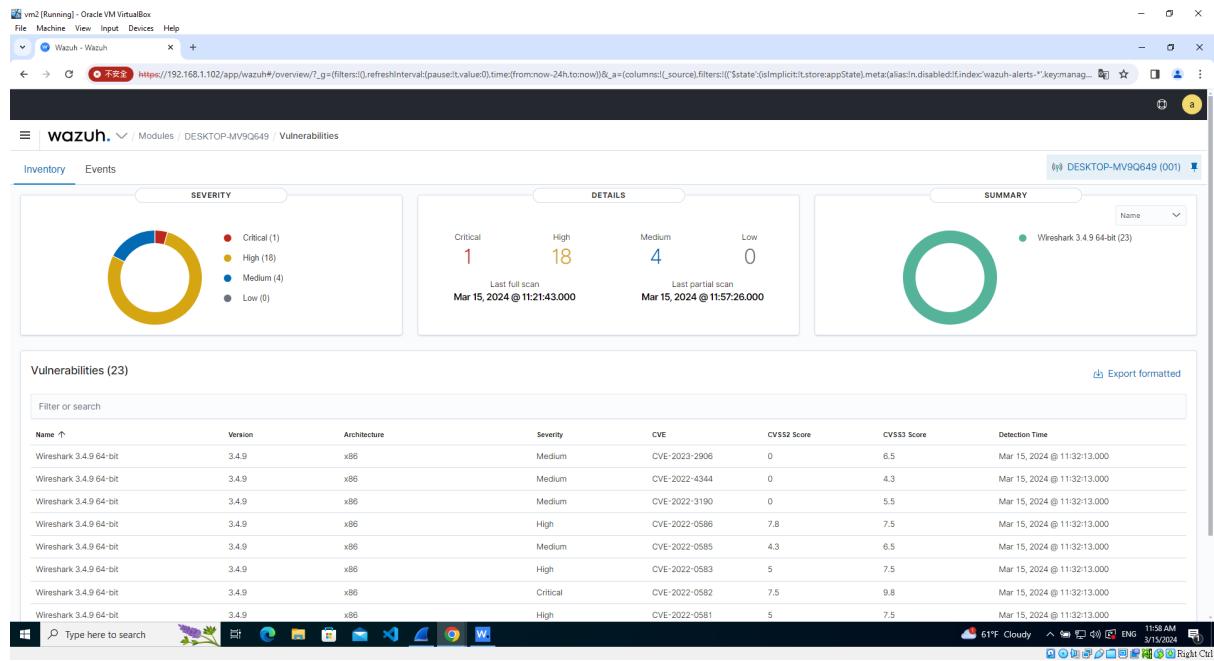
```
1 <!--
2   Wazuh - Manager - Default configuration for centos 7.9
3   More info at: https://documentation.wazuh.com
4   Mailing list: https://groups.google.com/forum/#!forum/wazuh
5 -->
6
7 <ossec_config>
8   <global>
9     <jsonout_output>yes</jsonout_output>
10    <alerts_log>yes</alerts_log>
11    <logall>no</logall>
12    <logall_json>no</logall_json>
13    <email_notification>no</email_notification>
14    <smtp_server>smtp.example.wazuh.com</smtp_server>
15    <email_from>wazuh@example.wazuh.com</email_from>
16    <email_to>recipient@example.wazuh.com</email_to>
17    <email maxperhour>12</email maxperhour>
```

Save    Restart Manager

Then, restart the service.



Last, go to Wazuh dashboard -> 'Vulnerabilities'. Here are the detection of vulnerabilities of the Windows machine.



## • Task 8 – Analyzing the Vulnerability Dashboard

The Wazuh Vulnerability Dashboard indicates a total of 23 vulnerabilities. One of them is critical, 14 are high-level vulnerabilities, and four are medium-level vulnerabilities. There is no low level of vulnerability. Furthermore, Wireshark affects the top five high-security vulnerabilities.

At the same time, finding fixes and recommendations for vulnerabilities is crucial. Here are the fixes and advice from the NIST and Wireshark official websites.

- CVE2022-0586:  
<https://nvd.nist.gov/vuln/detail/CVE-2022-0586>
- CVE-2022-0583:  
<https://nvd.nist.gov/vuln/detail/CVE-2022-0583>  
<https://www.wireshark.org/security/wnpa-sec-2022-03.html>
- CVE-2022-0581:  
<https://nvd.nist.gov/vuln/detail/CVE-2022-0581>  
<https://www.wireshark.org/security/wnpa-sec-2022-05.html>
- CVE-2021-4190:  
<https://nvd.nist.gov/vuln/detail/CVE-2021-4190>
- CVE-2021-4186  
<https://nvd.nist.gov/vuln/detail/CVE-2021-4186>

<https://www.wireshark.org/security/wnpa-sec-2021-16.html>

## Analysis:

During this capstone exercise, two reports were created in overall, one by task4 and the other by task6. Task 4 is a security events report that displays the target IP, the operating system version, and the version of the Wazuh server being utilized. Next, the report provides a concise overview of the warnings. The top three notifications in this example are 'Windows login success', 'Windows audit policy updated', and 'Windows User Logoff'. They have been recorded 19, 15, and 4 times. At the same time, this report also illustrates the evolution of alert groups. The most frequent sequence of elements is 'sca', which occurs 396 times.

Task 6 includes an integrity monitoring report. It displays notifications for file changes, such as rights, content, ownership, and attributes. Thus, the second section of this report displays the top three FIM rules, which include file uploaded to the system and file removed.

In addition, a dashboard was produced when the vulnerability analysis work was completed. There are a total of 23 vulnerabilities throughout the attack.

## Technical Challenges:

In this technical capstone practice, I faced two main technical challenges.

- Insufficient RAM on the Linux computer prevents the Wazuh-indexer service from working properly.

First, I created a virtual Linux computer with a two-core CPU and two gigabytes of RAM. However, the service would terminate after the machine had run for a time. I checked

the RAM utilization and discovered that it had reached 98%. Thus, I changed the settings to 2 cores and 4 GB of RAM, which resolved the problem.

- Cannot get the vulnerability.

After resolving the prior problem, I was still stuck on task 7 since the system was unable to discover any vulnerabilities throughout the night. Therefore, I endeavored to install Wireshark to monitor network traffic and identify any suspicious activity or anomalous behavior that could potentially stem from system vulnerabilities. After installing Wireshark, I was able to find the vulnerability and overcome the task.

## Learnings from Capstone:

This capstone project covers several significant trainings:

- To learn how to set up a virtual environment using a Linux machine and a Windows operating system. In addition, configure internal networking to link two VMs to each other.
- In this project, I learned how to set up Wazuh, an open source SIEM, as well as how to do log analysis, file integrity monitoring, and vulnerability detection. Knowing the tool may help strengthen the organization's or industry's cyber security posture.